# Synopsys Study Shows that Ninety-One Percent of Commercial Applications Contain Outdated or Abandoned Open Source Components

Analysis of more than 1,250 commercial codebases finds that open source security, license compliance, and operational risk remains widespread

MOUNTAIN VIEW, Calif., May 12, 2020 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today released the 2020 Open Source Security and Risk Analysis (OSSRA) report. The report, produced by the Synopsys Cybersecurity Research Center (CyRC), examines the results of more than 1,250 audits of commercial codebases, performed by the Black Duck Audit Services team. The report highlights trends and patterns in open source usage within commercial applications, and provides insights and recommendations to help organizations better manage open source risk from a security, license compliance, and operational perspective.

The 2020 OSSRA report reaffirms the critical role that open source plays in today's software ecosystem, revealing that effectively all (99%) of the codebases audited over the past year contain at least one open source component, with open source comprising 70% of the code overall. More notable is the continued widespread use of aging or abandoned open source components, with 91% of the codebases containing components that either were more than four years out of date or had seen no development activity in the last two years.

The most concerning trend in this year's analysis is the mounting security risk posed by unmanaged open source, with 75% of audited codebases containing open source components with known security vulnerabilities, up from 60% the previous year. Similarly, nearly half (49%) of the codebases contained *high-risk* vulnerabilities, compared to 40% just 12 months prior.

"It's difficult to dismiss the vital role that open source plays in modern software development and deployment, but it's easy to overlook how it impacts your application risk posture from a security and license compliance perspective," said Tim Mackey, principal security strategist of the Synopsys Cybersecurity Research Center. "The 2020 OSSRA report highlights how organizations continue to struggle to effectively track and manage their open source risk. Maintaining an accurate inventory of third-party software components, including open source dependencies, and keeping it up to date is a key starting point to address application risk on multiple levels."

A summary of the most noteworthy open source risk trends identified in the 2020 OSSRA report follows:

- **Open source adoption continues to soar.** Ninety-nine percent of codebases contain at least some open source, with an average of 445 open source components per codebase—a significant increase from 298 in 2018. Seventy percent of the audited code was identified as open source, a figure that increased from 60% in 2018 and has nearly doubled since 2015 (36%).
- **Outdated and "abandoned" open source components are pervasive.** Ninety-one percent of codebases contained components that either were more than four years out of date or had no development activity in the past two years. Beyond the increased likelihood that security vulnerabilities exist, the risk of using outdated open source components is that updating them can also introduce unwanted functionality or compatibility issues.
- **The use of vulnerable open source components is trending upward again.** In 2019, the percentage of codebases containing vulnerable open source components rose to 75% after dropping from 78% to 60% between 2017 and 2018. Similarly, the percentage of codebases containing high-risk vulnerabilities jumped up to 49% in 2019 from 40% in 2018. Fortunately, none of codebases audited in 2019 were impacted by the infamous Heartbleed bug or the Apache Struts vulnerability that haunted Equifax in 2017.
- **Open source license conflicts continue to put intellectual property at risk.** Despite its reputation for being "free," open source software is no different from any other software in that its use is governed by a license. Sixty-eight percent of codebases contained some form of open source license conflict, and 33% contained open source components with no identifiable license. The prevalence of license conflicts varied significantly by industry, ranging from a high of 93% (Internet & Mobile Apps) to a relatively low of 59% (Virtual Reality, Gaming, Entertainment, Media).

To learn more, download a copy of the 2020 OSSRA report, or register for our May 13 webinar, Lessons on Open Source Governance From the 2020 OSSRA Report.

**About the Synopsys Software Integrity Group**

Synopsys Software Integrity Group helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle. Learn more at www.synopsys.com/software.

**About Synopsys**

Synopsys, Inc. (Nasdaq: SNPS) is the Silicon to Software™ partner for innovative companies developing the electronic products and software applications we rely on every day. As the world's 15th largest software company, Synopsys has a long history of being a global leader in electronic design automation (EDA) and semiconductor IP and is also growing its leadership in software security and quality solutions. Whether you're a system-on-chip (SoC) designer creating advanced semiconductors, or a software developer writing applications that require the highest security and quality, Synopsys has the solutions needed to deliver innovative, high-quality, secure products. Learn more at www.synopsys.com.

**Editorial Contacts:**
Mark Van Elderen
Synopsys, Inc.
650-793-7450
mark.vanelderen@synopsys.com

SOURCE Synopsys, Inc.